Use Case Name	Domain	Schedule
“Low & Slow” Password Attack	Access	(0 6 * * 1) At 06:00 on Monday - Continuos Schedule
	Access	(0 5 * * 1) At 05:00 on Monday - Continuos Schedule
Terminated and Inactive Account Monitoring	Identity	(* 5 * * 1) At every 5th minute. Realtime Schedule
Successful Brute Force Attack followed with Exploitation	Endpoint	(*/15 * * * *) -At every 15th minute - Realtime schedule

Use Case Name	Domain	Schedule
Port scan or possible intrusion	NA	(*/60 * * * *) - At every 1 hour
	NA	(*/20 * * * *) - At every 20th minute
	NA	(*/20 * * * *) - At every 20th minute
	NA	(*/20 * * * *) - At every 20th minute
	N/A	(*/20 * * * *) - At every 20th minute
	N/A	(*/60 * * * *) - At every 1 hour
	N/A	(*/20 * * * *) At every 20th minute
Authentication sweep attack	Access	(* 5 * * 1) At every 5th minute. Realtime Schedule
	Access	(* 5 * * 1) At every 5th minute. Realtime Schedule

Use Case Name	Domain	Schedule
	Access	(* 5 * * 1) At every 5th minute. Realtime Schedule
Compromised Credentials	N/A	(Schedule type: Basic; Run every: day after midnight; Schedule Windows: 0; Schedule Priority: Default)
Attempt to Exploit certain Vulnerabilities	Network	(*/15 * * * *) -At every 15th minute - Realtime schedule
Potential Malware Outbreak	Endpoint	(*/20 * * * *) - At every 20th minute - Realtime schedule
	Endpoint	(*/20 * * * *) - At every 20th minute - Realtime schedule
Brute Force Attack Attempt to Remote Access systems	NA	(*/15 * * * *) - At every 15th minute
HX Exploit found	Endpoint	(*/20 * * * *) - At every 20th minute - Realtime schedule
HX IOC match found	Endpoint	(*/20 * * * *) - At every 20th minute - Realtime schedule

Use Case Name	Domain	Schedule
NX Attack Event	Endpoint	(*/20 * * * *) - At every 20th minute - Realtime schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Use Case Name	Domain	Schedule

Time Range	Description from SIEM logging extension	Required Logs
Start time: -7d@d; End time: now;	The goal of this use case is to detect attackers attempt to circumvent password lockout controls by slowly attempting password guesses on one or many accounts.	Cisco ASA (VPN Gateway)
Start time: -7d@d; End time: now;		Windows Security Log
Start time: -5m@s; End time: now;	When the account of a terminated employee is re-enabled and used (or attempted to be used), it can indicate the presence of a variety of different risks: shared account use, malicious disgruntled user, or potentially a breach by an outsider.	Windows Security Log
Start time: -15m; End time: now;	The goal of this use case is to monitor successful login after failed login followed by IoC matched or exploitation alert from EDR.	FireEye HX (or other endpoint detection and response product) Windows Security Log

Time Range	**Description from SIEM logging extension**	**Required Logs**
Earliest: -1h; End time: now;	The goal of this use case is to monitor Port scan performed on perimeter network by external/internal devices.	McAfee NIPS (or other Network IPS product)
Earliest: -20m; End time: now;		McAfee NIPS (or other Network IPS product) Threat Intelligence Product e.g. ThreatStream,
Earliest: -20m; Latest: now		Bluecoat (or other Proxy product) Threat Intelligence Product e.g. ThreatStream,
Earliest: -20m; Latest: now		Bluecoat (or other Proxy product) Threat Intelligence Product e.g. ThreatStream,
Earliest: -20m; Latest: now;		Bluecoat (or other Proxy product) Threat Intelligence Product e.g. ThreatStream,
Earliest: -1h; Latest: now;		Checkpoint (or other Firewall product) Threat Intelligence Product e.g. ThreatStream,
Earliest: -20h; Latest: now;		Checkpoint (or other Firewall product) Threat Intelligence Product e.g. ThreatStream,
Start time: -5m@s; End time: now;	The goal of this use case is to detect multiple failed login for multiple destination from single source IP within 5 minutes.	Cisco ASA (VPN Gateway)
		Windows Security Log

Time Range	Description from SIEM logging extension	Required Logs
Start time: -5m@s; End time: now;		Cisco ASA (VPN Gateway) Threat Intelligence Product e.g. ThreatStream, LookingGlass
Earliest: -1d; Latest: now;	The goal of the use case is to monitor the enterprise compromised email account reported by Threat Intelligence.	Threat Intelligence Product e.g. ThreatStream, LookingGlass
Start time: -15m; End time: now;	Network IPS detected any traffic signature on any internet facing servers with relevant vulnerabilities highlighted in the endpoint/server. Extract CVE field in both Network PS and Nessus using regex (built-in feature in the Splunk).	McAfee NIPS (or other Network IPS product) Vulnerability scan tool e. g. Tenable, Rapid7
Start time: -20m@m; End time: now;	The goal of this Use Case is to monitor multiple malware events from antivirus and/or endpoint protection on the multiple end-points within 20 minutes.	FireEye HX (or other endpoint detection and response product)
Start time: -20m@m; End time: now;		
Earliest: -15m@s; Latest: now;	Successful Brute Force Attack to Remote Access systems	Cisco ASA (VPN Gateway) Threat Intelligence Product e.g. ThreatStream, LookingGlass
Start time: -20m@m; End time: now;	The goal of this Use Case is to monitor malware events or alerts for 'exploit found' events.	FireEye HX (or other endpoint detection and response product)
Start time: -20m@m; End time: now;	The goal of this Use Case is to monitor malware events or Alerts for 'IOC match found' events.	FireEye HX (or other endpoint detection and response product)

Time Range	Description from SIEM logging extension	Required Logs
Start time: -20m@m; End time: now;	The goal of this Use Case is to monitor malware events or Alerts for 'Attack' events.	FireEye NX (or other Network Security Threat Prevention)

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Time Range	Description from SIEM logging extension	Required Logs

Search String
index=cisco_asa (process="%ASA-6-113015" OR process="%ASA-6-113005")| bucket _time span=1d | rex field=_raw "(?<user>user\s[=]\s[\w.]+)" | search user=* |stats count by user,_time | where count <3 | stats dc (_time) as dctime by user | where dctime > 6
index=windows sourcetype="WinEventLog:Security" EventCode=4625 (Logon_Type=2 OR Logon_Type=10) user!="*$" | bucket _time span=1d | stats count by user,_time| where count <3 | stats dc(_time) as dctime by user | where dctime >6
index=windows sourcetype="WinEventLog:Security" EventCode=4722 user!="*$" \| search [search index=windows sourcetype="WinEventLog:Security" (EventCode=4722 OR EventCode=4725) user!="*$" earliest=-7d latest=now | transaction user startswith="EventCode=4725" endswith="EventCode=4722" | table user] | table host, user
index=fireeye sourcetype=hx_cef_syslog (act="Detection ExD Hit" OR act="Detection IOC Hit") [search index=windows sourcetype="WinEventLog:Security" EventCode=4624 (Logon_Type=2 OR Logon_Type=10) user!="*$" [\|inputlookup failed_auth_tracker.csv \| where count>5 \| fields - count \| format] \|stats count by user,host \|rename host AS "src_host" \| table src_host] --> Search Driven Lookup : Failed Authentication Tracker index=windows source="WinEventLog:Security" EventCode=4625 user!="*$" (Logon_Type=2 OR Logon_Type=10 OR Logon_Type=4) | stats count by user, host | outputlookup failed_auth_tracker.csv

Search String
index=mcafee_nips (status!="Smart Blocked" AND status!="Attack Blocked") direction=Inbound | search [|`ts_ioc_search_sev(srcip, *, *, 90, *high, -30d@d, now)`| rename Indicator as src_ip | table src_ip | format]
index=mcafee_nips (status!="Smart Blocked" AND status!="Attack Blocked") direction=Outbound| search [|`ts_ioc_search_sev(srcip, *, *, 90, *high, -30d@d, now)`| rename Indicator as dest_ip | table dest_ip | format]
index=bcoat_logs sourcetype=bluecoat:proxysg:access:file (sc_filter_result="PROXIED" OR sc_filter_result="OBSERVED") | search [|`ts_ioc_search_sev(domain, *, *, 90, *high, -30d@d, now)`| rename Indicator as s_supplier_name | table s_supplier_name | format]
index=bcoat_logs sourcetype=bluecoat:proxysg:access:file (sc_filter_result="PROXIED" OR sc_filter_result="OBSERVED") | search [|`ts_ioc_search_sev(srcip, *, *, 90, *high, -30d@d, now)`| rename Indicator as s_supplier_ip | table s_supplier_ip | format]
index=bcoat_logs sourcetype=bluecoat:proxysg:access:file (sc_filter_result="PROXIED" OR sc_filter_result="OBSERVED") | search [|`ts_ioc_search_sev(url, *, *, 90, *high, -30d@d, now)`| rename Indicator as cs_uri_query | table cs_uri_query | format]
index=checkpoint sourcetype=opsec action=allowed direction=inbound | search [|`ts_ioc_search_sev(srcip, *, *, 90, *high, -30d@d, now)`| rename Indicator as src_ip | table src_ip | format]
index=checkpoint sourcetype=opsec action=allowed direction=outbound | search [|`ts_ioc_search_sev(srcip, *, *, 90, *high, -30d@d, now)`| rename Indicator as dest_ip | table dest_ip | format]
index=cisco_asa (process="%ASA-6-113015" OR process="%ASA-6-113005") | stats values(IP) as src_ip, count values(server) dc(server) as dcvalue by IP| where dcvalue>1 | rename values(server) as dest | fields src_ip, dest
index=windows sourcetype="WinEventLog:Security" EventCode=4625 Logon_Type=10 | stats values(Source_Network_Address) as src_ip, count values(dvc) dc(dvc) as dcvalue by Source_Network_Address | where dcvalue>1 | rename values(dvc) as dvc | fields src_ip, dvc

Search String
index=cisco_asa (process="%ASA-6-113015" OR process="%ASA-6-113005") | search [|`ts_ioc_search_sev(srcip, *, *, 90, *high,  -30d@d, now)`| rename Indicator as IP | table IP | format] | stats values(IP) as src_ip, count values(server) dc(server) as dcvalue by IP| where dcvalue>1 |rename values(server) as dest | fields src_ip, dest
|`ts_ioc_search(email, *@xxx.com.sg, *, 90, -1d@d, now)` | rename Type as threat_category, Indicator as threat_match_value, Source as threat_source_id ***Replace xxx with the enterprise email address*
index=tenable cve=* earliest=-30d latest=now | search [search index=mcafee_nips *CVE* direction=Inbound (status!="Smart Blocked" AND status!="Attack Blocked") earliest=-15m latest=now | rex field=Attack_Name "(?<cve>CVE-\d{1,5}-\d{1,5})" | rename DIP as ip | stats count by ip, cve | fields - count]
index=fireeye sourcetype=hx_cef_syslog (act="Detection ExD Hit" OR act="Detection IOC Hit") | stats count values(dhost) dc(dhost) as dcvalue by cs4 | where dcvalue>4 | table values(dhost), cs4 | rename values(dhost) as host, cs4 as threat_description
index=fireeye source=hx act=”Detection IOC Hit” | stats count values(dhost) dc(dhost) as dcvalues by cs4 | where dcvalue>4 | table values(dhost), cs4 | rename values(dhost) as host, cs4 as threat_description
index=cisco_asa (process="%ASA-6-113015" OR process="%ASA-6-113005" OR process="%ASA-6-113004" OR process="%ASA-6-113012" OR process="%ASA-6-315013") IP=* | stats count by IP | where count >4 | search [|`ts_ioc_search_sev(srcip, *, *, 90, *high, -30d@d, now)`| rename Indicator as IP | table IP]
index=fireeye sourcetype=hx_cef_syslog category="ExD Hit Found" | eval rawlog=_raw | table _time, src_dns, src_ip, dhost, rawlog, ioc_name, categoryTupleDescription | rename values(src_dns) as dest, dhost as host, categoryTupleDescription as threat_description
index=fireeye sourcetype=hx_cef_syslog (category="IOC Hit Found" OR category=”ExD Hit Found”) | eval rawlog=_raw | table _time, src_dns, src_ip, dhost, rawlog, ioc_name, categoryTupleDescription | rename values(src_dns) as dest, dhost as host, categoryTupleDescription as threat_description

Search String
index=fireeye sourcetype=fe_cef_syslog category="*" | eval rawlog=_raw | table _time, cef_name, id, cs4, signature, request, src_nt_host, src_ip, rawlog, transport, src_dns, dvc_host | rename values(src_dns) as dest, cef_name as threat_description, src_nt_host as host, transport as protocol, request as url

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

Search String

